XRAY Beamline Services

Computing and Network Resources for XSD Beamlines

David Wallis and Kenneth Sidorowicz

6/3/2013

The APS Engineering Support Division's Information Technology Group maintains and supports the APS computing infrastructure including the management of all APS enterprise networks and CAT backbone networks, tier 2 firewalls, servers, storage and printers in conjunction with supporting all Laboratory cyber security policies. This document provides an overview of the IT services available to the XSD beamlines. For additional information please see the IT home page http://www.aps.anl.gov/it.

Contents

1 Sector Liaison

A liaison from the IT group is assigned to each XSD sector. See http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/staff/ under "Liaison" for the current sector assignments.

The IT liaison is intended to serve as a conduit for information between the IT group and each sector. Sector liaisons should meet with their assigned sectors from time to time to discuss IT needs in the sector, as well as to keep the sector up to date on short and long term IT plans. The sector liaison is also a resource for each sector, and can help to expedite the resolution of urgent problems at a sector.

2 Networking Services

APS provides each sector with a public class C IP subnet which can be shared between the beamline and office computers. All beamline network jacks are wired using CAT 6A-rated cabling supporting communications up to 10Gbps. The network cabling is connected to either a dedicated network switch/router on the beamline or a shared switch/router in the LOM for the offices. These network switches currently support 1Gbps connections to the desktops and multiple 10Gbps connections to the APS backbone.

Each beamline is assigned a dedicated name server, DHCP server, NTP server and PV-Gateway interface. These services are local to the beamline so they will always be available in the event of an upstream network failure. All computers must be registered with the IT group before they will be assigned a static IP address. Computer information is uploaded at night to the Lab network database as required by DOE. All computers will be subject to daily short network scans and monitoring. Full network scanning only occurs during shutdown periods for the beamlines..

To maintain the integrity of the network and to centrally manage every network port, mini-switches are discouraged on the beamline networks. By having all devices connected directly to the beamline switch network administrators are able to diagnose and troubleshoot problems in a shorter amount of time and minimize downtime due to failed devices on the network. If sufficient network jacks are not available in a desired beamline location, please contact IT support so additional jacks can be installed.

2.1 Visitor Network/Wireless

APS provides a wireless 802.11g/n network for visiting or wireless users. Wireless computers must register before connecting to the network by starting a Web browser and filling out the form that is automatically displayed. See http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/Networking/?page=registration for additional information. Wired visitor network connections are also available. The visitor network is separated from the APS network through a firewall and has no access to the internal network.

2.2 Firewall

APS manages a tier 2 firewall to provide security for our network users. All network protocols inbound and outbound are by default blocked. Various outbound protocols such as web, email, SSH and other common protocols have been enabled for all users. Inbound firewall access (conduits) requires approval from the Laboratory IT-ARG committee. Contact IT Support if you have questions

about firewall rules. When using a Web browser behind the firewall, access to URLs and references to non-standard ports (for example, port 8080) will NOT work. See http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/Networking/?page=APSproxy for information on how to configure the web proxy.

Argonne CIS manages the tier 1 firewall which connects the Lab to the Internet. Coordination of conduits between the two firewalls is managed by the IT-ARG and the CIS and APS network administrators.

2.3 Spam Email

Argonne CIS manages a pair of anti-spam appliances that quarantine spam and permit users to manage their own spam. These devices are Cisco's IronPort appliances. They are integrated appliances that protect you from spam, viruses, phishing attacks, zombies and hackers. They even protect against threats that haven't been identified yet. Each user has the ability to view spam email that has been quarantined and the options to release, delete or whitelist known good senders. If any of your incoming email is quarantined as spam an email message will be sent to your email account at 6:00 am with the subject of "Argonne Anti Spam Notification". This email will contain a listing of all your email quarantined for that day. See the Spam FAQ http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/CyberSecurity/index.php?page=spamfaq for additional information.

In addition all email flows through the Department of Homeland Security's Enhanced Computer Security Project (0DEX). See http://inside.anl.gov/news/archives/2013/01/dex-will-help-protect-labs-computers for additional information.

2.4 Web URL Filtering

APS uses SmartFilter from McAfee to automatically categorize each web site and filter web access based on these categories. The restricted categories, selected by APS upper management, are deemed to have no direct relevance to any work to be performed in support of the APS mission. They are also deemed to provide or display material considered controversial in nature by significant sectors of the general public. This function was enabled to help ensure adherence to the Argonne and APS computer use policy as well as to prevent embarrassment to DOE, Argonne and APS through the publication of lists of sites that access these web pages. Argonne considers the sites in the restricted access categories to be non-business related and unproductive for most employees in the Argonne business environment. The lists used are updated daily from a service set up for this purpose.

2.5 Private Networks

The IT group can assist sectors in setting up private networks on the beamline for special projects or equipment that needs to be isolated from public networks.

2.6 Visiting Computers

Normally, only APS computers can be connected to APS internal networks. In cases where visiting scientists need to bring their own computer equipment to operate their experiment, the IT group can assist the beamline to support such an arrangement.

3 Computer Accounts

A web link is available on the IT home page (http://www.aps.anl.gov/it) to request a computer account.

3.1 ANL Domain Account

An ANL Domain account is required for access to Windows computers in the CLO and some XSD LOMs, access to the APS Citrix server, and for VPN network access.

3.2 XRAY Domain Account

An XRAY Domain account is required to access XSD Windows computers on the Experiment Floor.

3.3 APS Operations Account

An APS Operations account is required to access oxygen and phoebus client workstations, the ICMS document management system, as well as Linux, Macintosh, or Solaris computers on the Experiment Floor.

3.4 Local Administration

APS/IT recognizes that Windows-based PC workstations are an integral and important part of many beamlines and experiments, and those PCs, by nature, require certain operations to be performed by a user with administrator privileges. This section documents the policies and procedures required for beamline personnel to have local administrator access to their PCs.

1. Who can be a local PC administrator

    - Each sector may designate up to two staff members as local PC administrators.
    - Specific training classes may be required in the future.

2. What workstations are eligible for local administration privileges
   Windows Computers running experiments on the beamline floor may have local administrator accounts if they fall under certain criteria outlined below:

    - The PC must be connected to and users authenticated to the XRAY domain
    - The PC must be used expressly for the purpose of facilitating an experiment
    - The PC will not be used at any time as a regular desktop workstation.

Local PC administration Best Practices

If the computer fulfills the requirements detailed above, the designated sector administrator may request a local administrator account for that computer.

Rules for local administrator accounts:

- Never give out the local admin account. As the sector administrator, you are responsible for ALL activity performed on that computer under the local administrator account.

- DO NOT treat the local admin account as a regular user account. Use a user account for all activities, log in as local admin ONLY when an action requires administrative privileges.
- Use the RUN AS command for most of your administrative needs. Software installation, driver installation, and other common admin tasks can be performed in a regular user account, elevated to admin by the RUN AS command.
- Local administration privileges are to be used only for emergencies that affect beamline operations when IT staff is not available to fix the problem
- Changes made to a PC by a local admin must be documented in an email to IT Support within a reasonable time frame. APS uses automated configuration management tools, and undocumented changes could be deleted by the tools.

4 Beamline Services

4.1 Local Data Storage (Tier 1)

The disk storage attached to the beamline detectors and computers is considered tier 1 storage. Many beamlines find it useful or necessary to store data collected from experiments on local disks or higher performance disk arrays. The IT group can assist in setup and configuration of local storage as required by the experiments on a beamline. Please notify IT when user data on local disks needs to be backed up. While the system disks are automatically backed up additional drives and arrays must be entered into the backup system configuration.

4.2 NFS (Tier 2)

The primary method of accessing files in XSD is via NFS from Linux, Mac, and Solaris workstations. The primary file servers are the sector distributed servers (dservs) configured to provide a virtual server (named “sec#” where ‘#” is the sector number) for each XSD beamline. The IT group currently manages approximately 1 Petabyte of disk storage for XSD beamlines. This includes shared/general purpose storage (user home directories, software distribution, etc), as well as storage dedicated to beamline data storage and backup disk arrays.

4.3 Samba (Tier 2)

Access to XSD file systems on the dserv servers is provided to Windows computers via the Samba software. Samba allows Windows users to browse the XSD file systems as if they were on a Windows server. Users can browse to the primary XSD file servers, or can access them directly (e.g., “\\<server_name>\<share_name>” from the “Start/Run” option).

4.4 Backups

4.4.1 Linux and Solaris

IT provides a centralized file backup and restore system. All data on the XSD servers (user home directories, scientific data shares, etc) are backed up according to the following schedule:

Tuesday – full backup

Wednesday – Monday – incremental backup

In general, data on individual Linux and Solaris workstations are not backed up – files should be copied from a workstation's local disk to space on a primary file server. Contact IT for backups of Linux systems.

4.4.2 Windows

The XSD Windows computer backup system will allow XSD staff to initiate backups for selected data on beamline computers when the systems are not engaged in operating an experiment. This allows the PCs to be backed up in a way that doesn't impact beamline data acquisition or experiment operation.

4.5 Web Servers

There are several web server options for beamlines at the APS. For a public web presence, the preferred standard is to use the primary APS web server, with a URL such as "http://www.aps.anl.gov/Sectors/SectorN". For non-public, experiment specific or operational information and control, IT maintains an Apache web server that provides a virtual domain for each sector or station, with URLs similar to "http://sectorN.xray.aps.anl.gov" or "http://Nid.xray.aps.anl.gov".

Each beamline that desires one can have a virtual domain created on the XSD web server. Each sector's virtual server is self-contained, and provides a private cgi-bin directory, database support, and more. Each sector has full control over their server, and can manage their documents and web applications as they see fit.

The XSD web server provides a rich web environment, including the following features:

PHP 5

MySQL 5

Private CGI-BIN directory

Perl

Python

Elog electronic logbook

Elog read-only mirror sites

Contact IT Support if you are interested in setting up a web presence for your beamline or station.

4.6 Distributed Network Services

IT provides a number of servers, known as "dserv" (distributed services) servers. These servers are dedicated to APS beamlines (both XSD and non-XSD) and provide the following network services:

- DNS (name service)
- DHCP (dynamic host configuration protocol)
- NTP (network time protocol)
- FTP (file transfer protocol) for booting IOCs

- NFS (for beamline home directories, /APSshare and other IOC-specific file systems)
- SAMBA (for Windows access to the same file systems)

The dserv servers have network interfaces directly connected to each beamline subnet, so that their services will be available even in the event of a central network failure. For XSD sectors, the dserv provides the boot and operational data for IOCs, storing the IOC configurations as well as automatically saved operational data.

4.7 Subversion/Trac

IT provides a Subversion version control server (https://subversion.xray.aps.anl.gov), along with the Trac (http://trac.edgewall.org) project management software. Contact APS IT Support if you would like to have a Subversion repository and/or Trac environment set up.

4.8 Commercial/Licensed Software

The following commercial/licensed software is available for XSD Solaris clients:

- IDL
- Mathematica
- Matlab
- Spec

4.9 Open Source and Other Software

IT supports a wide variety of commercial, third party and open source software for use by XSD personnel and beamline users. At this time we are supporting over 2000 software applications on all platforms..

4.10 Detector Pool

The XSD division maintains a set of detectors that are available for loan to beamlines. The detectors are registered in the IT Equipment Tracking System and will automatically receive an IP number on any XSD beamline network.

4.11 Email List Service

APS maintains a Mailman email list server to facilitate communication and collaboration among APS users. The list server can be accessed via the web at: http://www.aps.anl.gov/mailman/listinfo. The main list server page describes the currently available email lists. Note that some lists have a closed membership, and some are "broadcast only" lists, rather than discussion lists. Contact IT support if you would like to create additional lists.

4.12 IOC Console Access

APS-IT and the BCDA group maintain a service that provides uniform and controlled access to the consoles of XSD beamline IOCs. Network terminal servers are installed in each XSD sector, and provide serial TTY connections to the console port of each IOC at the beamlines in that sector. A program, called “iocConsole”, allows beamline users to connect remotely to any of the consoles. The iocConsole program also provides some history of the output of each IOC console, even when nobody is connected to it. The BCDA group maintains access controls for the iocConsole software that allows

users to access only those IOCs they are authorized to access.

5 Outside Access to XSD Networks

5.1 VPN

VPN (Virtual Private Network) access to XSD computers is available via the APS VPN network. VPN access requires an ANL domain account, and must be enabled for each account. VPN access cannot be enabled for group (shared password) accounts. The main VPN server for the APS and XSD is visa.aps.anl.gov.

5.2 SSH

IT provides multiple SSH servers for accessing XSD beamline computers from outside the APS. The name which accesses the servers is “xgate.xray.aps.anl.gov”.

SSH access uses an APS Cryptocard keyfob. You must submit a Support Request for a Cryptocard for external XSD SSH access. Accounts that have had external SSH enabled, but don't use it for 12 months, will have that access removed from their account per Lab policy. External SSH access cannot be enabled for service (shared password) accounts.

Additionally, IT provides SSH access from the Argonne Guest House for non-APS users who are conducting experiments on XSD beamlines. This service allows a user to connect to beamline computers using common SSH software and an account name and password that will be supplied by the beamline contact.

5.3 FTP

IT provides an anonymous FTP server to allow non-APS users to transfer experiment data to their home institution, or to a laptop computer they bring with to the APS. The FTP server is named “ftp.xray.aps.anl.gov.” File repositories are created for each user or experiment station. Contact IT Support to have an FTP repository set up for your experiment.

Due to the amount of disk space required, files left on the XSD FTP server are automatically purged after 14 days. If you require files to be available longer than that, the limit can be increased on a per-user basis.

5.4 GridFTP

GridFTP is a high-performance, reliable data transfer protocol optimized for high-bandwidth wide area networks. It's based on the FTP protocol and defines extensions for high-performance operation and security. It's standardized through Open Grid Forum (OGF). GridFTP is the OGF recommended data movement protocol.

Globus-url-copy is the most commonly used client for GridFTP. It's syntax is as follows: globus-url-copy [options] srcURL dstURL The URL rules are: protocol://[user:pass@][host]/path
host can be anything resolvable - IP address,localhost, DNS name

For additional information please refer to: http://www.globus.org/toolkit/

The two GridFTP servers available at the APS are:

Wolf.xray.aps.anl.gov	Internal transfers to/from Orthros
Clutch.xray.aps.anl.gov	External transfers to/from Orthros

6 Supporting Beamline Users

6.1 Data transfer

Data transfer to storage systems such as memory sticks and USB-hard drives is often necessary in order to move large volumes of data offsite. Please contact the IT group if there are any problems during the process.

Data transfers to home institutions are possible via ftp through ftp.xray.aps.anl.gov or via GridFTP through clutch.xray.aps.anl.gov. The recommended solution for GridFTP is to use Globus Online. See Globus Online section in the HPC Users wiki https://wiki.aps.anl.gov/hpcu/index.php/Main_Page

7 PC/Workstation/Laptop Configurations

The IT Support group maintains a list of supported hardware configurations for PCs and Workstations at the APS:

http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/Services/SupportedHardware/

Supported desktops, workstations, and laptops are from the business catalogs at Hewlett-Packard and Dell.

As part of Lab configuration management requirements the APS requires that you purchase from the recommended platform list unless you have a specific requirement due to vendor hardware limitations for beamline equipment, which the recommended systems do not provide. In that case, you must contact the IT Support group leader to have your hardware requirements reviewed.

You can contact the IT Support group if you would like assistance choosing PC/workstation/laptop hardware configurations.

8 Getting Help

8.1 Support Request System

IT Support uses a web-based database tool called Remedy to manage and monitor Support Requests from all APS users. Users are asked to create a Support Request case whenever they need IT Support help. Using the Support Request system helps ensure that requests does not get lost, and allows IT Support personnel to monitor response time, discover trends, and prioritize work. Using the Support Request system also helps ensure that requests are quickly seen by the proper support personnel, even if the IT staff the user normally work with is out sick or away on vacation. This system also allows the user or requester to monitor their cases, view who the case is assigned to and also view the work log.

The Support Request system can be accessed from any platform using Firefox as the suggested web browser at: http://www.aps.anl.gov/hd. The user should login with their APS Operations account username. If they don't have one or this fails, the user should click on Logout, then try again with their badge #. If this still fails, they should click on Logout and call 2-9700 during business hours.

8.2 Out-of-hours support

IT Support provides support for critical applications outside of normal work hours. Out-of-hours support is limited to emergencies that affect the operation of beamline experiments.

Non-APS beamline users should contact their beamline contact person for any problems they experience. Your beamline contact may be able to resolve the problem directly, or escalate the problem to the IT group if necessary.

APS beamline users or staff should contact the on-duty Floor Coordinator (x2-0101) for out-of-hours problems. If a Floor Coordinator is not available, they should contact the Main Control Room (x2-9424) directly.

The Floor Coordinator or MCR operator will evaluate the problem, and let the user know if their problem is related to a known issue (such as a network outage). Otherwise, they will contact the proper on-call IT Support staff member. The IT Support staff member will contact you via phone to further evaluate the problem.

8.3 Critical Problems

Whenever a critical problem occurs – one that affects the operation of a beamline or experiment, IT Support should be contacted directly, and then a Support Request case should be opened. During normal business hours (Monday through Friday, 8 am to 5 pm), users may call the IT Group Support number (252-9700). If outside normal business hours, the procedure for out-of-hours support listed above should be followed.

If it is known which IT Support staff member may be able to best resolve the problem, the user may also contact that person directly during regular business hours. Users should also remember to open a Support Request case for the problem to ensure the problem is logged

9 Communication to Beamlines

9.1 System Status Information

The IT Support Group maintains a web page that displays a summary of current network and server operational status. The URL of the page is http://status.aps.anl.gov. The web page is updated to inform users of current network or computer resource issues that may affect them. This page can also be seen on the site-wide TV system.

9.2 Email Notifications

The IT Group will periodically send out broadcast email message to alert users to ongoing problems, or to issue advanced notice of scheduled downtime or maintenance. These messages are sent to every account holder on APS and/or XSD beamline systems.

The emails are also archived and available on the web, with a link to the archived message included in the email message. You can access the complete archives at:

APS messages: http://www2.aps.anl.gov/info/

9.3 Monthly XSD/IT/BCDA/SSG Meetings

Monthly meetings with XSD and the IT, BCDA and SSG groups are held the fourth Tuesday of each month at 3:00 pm in LOM 431-C010. Chris Jacobsen is in charge of these meetings and the agenda. If you are interested in anything specific to be reported, contact Chris to have your issue or question added to the agenda.

9.4 IT Workshops

Members of the IT group will give workshops on specific topics such as remote access to the APS throughout the year. Notices of upcoming workshops are sent to the email notification lists.

9.5 Support Request System

One final method of communication between the IT group and beamline personnel is via IT's response to Support Requests, either by email, phone, or in-person help. The Support Request system can be accessed through your browser at http://www.aps.anl.gov/hd.